

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-124955

(43)Date of publication of application : 28.04.2000

(51)Int.Cl.

H04L 12/56
H04L 12/40
// H04K 3/00

(21)Application number : 10-296522

(71)Applicant : NEC CORP

(22)Date of filing : 19.10.1998

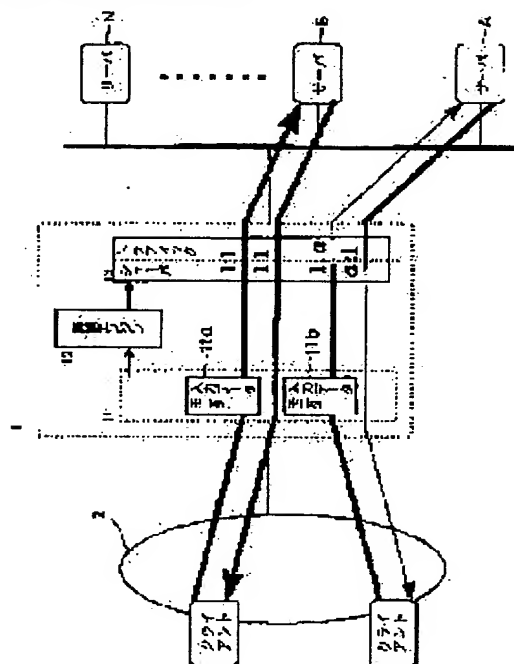
(72)Inventor : HASHIMOTO JUNJI

(54) NETWORK ATTACK PROTECTION SYSTEM FOR TRAFFIC SHAPING

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a network attack protection system which can be effective to the attack by a scanner attacking totally, can unnecessitate the change of a server program and can quickly respond to the contents of the attack.

SOLUTION: Communication data transmitted from an external network 2 are sampled by input data monitors 11a and 11b. When an inference engine 12 detects matching between the pattern of communication data sampled by these input data monitors 11a and 11b and an attack pattern stored in the inference engine 12, the rate α of shaping traffic with a traffic shaper 3 is controlled.



LEGAL STATUS

[Date of request for examination] 19.10.1998

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 3309961

[Date of registration] 24.05.2002

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-124955

(P2000-124955A)

(43) 公開日 平成12年4月28日 (2000. 4. 28)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード (参考)	
H 0 4 L	12/56	H 0 4 L 11/20	1 0 2 E	5 J 1 0 4
	12/40	H 0 4 K 3/00		5 K 0 3 0
// H 0 4 K	3/00	H 0 4 L 11/00	3 2 0	5 K 0 3 2

審査請求 有 請求項の数 5 O L (全 5 頁)

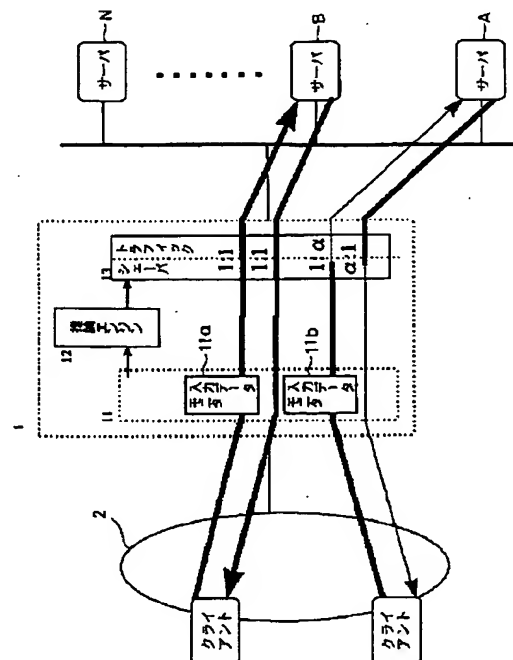
(21) 出願番号	特願平10-296522	(71) 出願人	000004237 日本電気株式会社 東京都港区芝五丁目7番1号
(22) 出願日	平成10年10月19日 (1998. 10. 19)	(72) 発明者	橋本 淳二 東京都港区芝五丁目7番1号 日本電気株式会社内
		(74) 代理人	100089875 弁理士 野田 茂
		Fターム (参考)	5J104 AA12 AA41 PA07 5K030 GA15 HC01 HC14 LC02 LC11 5K032 AA08 CC05 EA06

(54) 【発明の名称】 トラフィックシェーピングによるネットワーク攻撃防御システム

(57) 【要約】

【課題】 網羅的に攻撃をかけるスキャナなどの攻撃に有効、かつサーバプログラムの変更を不要にでき、攻撃の内容に即応できるトラフィックシェーピングによるネットワーク攻撃防御システムを提供すること。

【解決手段】 入力データモニタ11a, 11bにより外部ネットワーク2から伝送される通信データを採取する。この入力データモニタ11a, 11bで採取した通信データのパターンと推論エンジン12に記憶されている攻撃パターンとがマッチングしていることを推論エンジン12で検出すると、トラフィックシェーパ13によりトラフィックをシェーピングする割合 α を制御する。



BEST AVAILABLE COPY

【特許請求の範囲】

【請求項1】 外部ネットワークからの通信データを採取する入力データモニタと、

コンピュータへのアタックパターンがあらかじめ記憶され、上記入力データモニタより採取された上記通信データのパターンを検出して、その検出した上記通信データのパターンが上記記憶したアタックパターンとのマッチングの有無により上記通信データが上記コンピュータへのアタックであるか、否かの判断をする推論エンジンと、

上記推論エンジンが上記通信データのパターンから上記コンピュータへのアタックパターン検出時にトラフィックをシェーピングする割合を制御するトラフィックシェーパと、

を備えることを特徴とするトラフィックシェーピングによるネットワークアタック防御システム。

【請求項2】 上記トラフィックシェーパは、上記推論エンジンによる上記通信データのパターンと上記アタックパターンのマッチング検出時にトラフィックをシェーピングする割合 α を既定値 ($0 < \alpha < 1$) とすることを特徴とする請求項1記載のトラフィックシェーピングによるネットワークアタック防御システム。

【請求項3】 上記トラフィックシェーパは、上記推論エンジンによる上記通信データのパターンと上記アタックパターンのマッチング検出時にクライアントからサーバへのデータを α 倍にすることを特徴とする請求項1記載のトラフィックシェーピングによるネットワークアタック防御システム。

【請求項4】 上記トラフィックシェーパは、上記推論エンジンによる上記通信データのパターンと上記アタックパターンのマッチング検出時にサーバからクライアントへのトラフィック量を α 倍にすることを特徴とする請求項1記載のトラフィックシェーピングによるネットワークアタック防御システム。

【請求項5】 上記トラフィックシェーパは、上記推論エンジンにより検出したアタックの発信元である上記通信データが終了するとトラフィックをシェーピングする割合 α を元の既定値 ($0 < \alpha < 1$) に戻すことを特徴とする請求項1記載のトラフィックシェーピングによるネットワークアタック防御システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、トラフィックのシェーピングを行い、次のホストコンピュータ（以下、ホストと略称する）へのアタックへの移行時間を引き延ばすことにより、他のホストへのアタック時間を引き延ばすことができ、ホストへのアタックの解析が可能になり、アタックする犯人を特定するための情報を得ることができるようにしたトラフィックシェーピングによるネットワークアタック防御システムに関する。

【0002】

【従来の技術】 インターネットなどのパブリックネットワークの普及に伴い、ネットワーク経路による情報の盗難や不正利用などの犯罪が急増している。インターネットでは、不正アクセスのためのプログラムが流通しており、網羅的にアタックし、セキュリティホールを発見しようとするツールが数多く存在する。現在、これらのアタッキングツールやアタッカへの対策が急務であり、その対策に種々の試みがなされている。

【0003】 たとえば、特開平02-302139号公報には、複数のネットワーク間の接続部に通信データの発信先アドレスと発信元アドレスをチェックし、アクセス権を記録した内容にしたがって、不正アクセスを遮断する不正アクセス防止手段を備えたネットワークセキュリティが開示されている。

【0004】 また、LANあるいは公衆網などの伝送媒体に構築されるネットワークシステムにおいて、管理装置がアラーム情報と各中継装置が有するアクセス履歴情報とから不正アクセスをした端末装置が各中継装置のどちら側のポートに接続されているかを絞り込んでいくことにより、不正アクセスをした端末装置がどのLAN上で接続されているかを特定するセキュリティ方式が開示されている。

【0005】

【発明が解決しようとする課題】 しかしながら、これらの公報の場合には、いずれもホストへのアタックに対する直接的な対策とはならない。このような従来のネットワークアタック防御システムの課題を挙げると、以下のごとくである

【0006】 すなわち、従来は網羅的にインターネット上のサーバに対して「ポートスキャン」などを行われた場合、パケットフィルタリングなどにより、これらのアクセスを「遮断する」アイデアは存在した。しかし、この場合、アクセスを遮断することは即座に次のアタックに切り替わるきっかけとなってしまうことが多いため、アタッカは短時間でサービスポートなどを検出することができ、かつ迅速に次のアタックへ移行することができてしまうという課題がある。

【0007】 また、従来のアタックを遮断する方法もあるが、この方法では、攻撃元とのコネクションがすぐに切れてしまうことになり、攻撃元が次にどんなアタックを行うかを予想することが難しいという課題がある。

【0008】 この発明は、上記従来の課題を解決するためになされたもので、サーバ1台当たりのアタック時間を長くすることができ、網羅的にアタックをかけるスキャンなどの攻撃に有効かつ、サーバプログラムの変更を不要にでき、サーバに検出モジュールの導入を不要にできるとともに、アタックの内容に即した対応が可能となるトラフィックシェーピングによるネットワークアタック防御システムを提供することを目的とする。

【0009】

【課題を解決するための手段】上記目的を達成するために、この発明によるトラフィックシェーピングによるネットワーク攻撃防御システムは、外部ネットワークからの通信データを採取する入力データモニタと、コンピュータへの攻撃パターンがあらかじめ記憶され、上記入力データモニタより採取された上記通信データのパターンを検出して、その検出した上記通信データのパターンが上記記憶した攻撃パターンとのマッチングの有無により上記通信データが上記コンピュータへの攻撃であるか、否かの判断をする推論エンジンと、上記推論エンジンが上記通信データのパターンから上記コンピュータへの攻撃パターン検出時にトラフィックをシェーピングする割合を制御するトラフィックシェーパとを備えることを特徴とする。

【0010】この発明によれば、入力データモニタにより外部ネットワークから伝送される通信データを採取すると、この採集された通信データのパターンを推論エンジンにより検出される。検出された通信データのパターンが推論エンジンであらかじめ記憶されているコンピュータへの攻撃パターンとのマッチングの有無を検出し、その検出の結果、攻撃パターンと通信データのパターンがマッチングしていると判断すると、トラフィックシェーパにより、トラフィックをシェーピングする割合 α を制御する。

【0011】したがって、この発明では、サーバ1台当たりの攻撃時間を長くすることができ、網羅的に攻撃をかけるスキャナなどの攻撃に有効かつ、サーバプログラムの変更を不要にでき、サーバに検出モジュールの導入を不要にできるとともに、攻撃の内容に即した対応が可能となる。

【0012】

【発明の実施の形態】以下、この発明によるトラフィックシェーピングによるネットワーク攻撃防御システムの実施の形態について図面に基づき説明する。図1はこの発明の第1実施の形態の構成を示すブロック図である。この図1において、この第1実施の形態は防御装置1を備えている。クライアントX、YとコンピュータとしてのサーバA、B、・・・Nには特別な仕組みは必要ない。

【0013】防御装置1は、外部ネットワーク2からの通信データを採取する入力データモニタ11a、入力データモニタ11bによって得られた通信データのパターンを検出し、攻撃かどうかを判断する推論エンジン12と、トラフィックをシェーピングする割合を制御するトラフィックシェーパ13とにより構成される。推論エンジン12はあらかじめ攻撃パターンを記憶しており、推論エンジン12により入力データモニタ11a、入力データモニタ11bによって検出された通信データのパターンと攻撃パターンがマッチングしてい

ることを検出することにより、攻撃を検出する。トラフィックシェーパは攻撃検出時にトラフィックをシェーピングする割合 α ($0 < \alpha < 1$)を記憶している。

【0014】次に、以上のように構成されたこの第1実施の形態の動作について図2のフローチャート沿って説明する。図2のステップS1では、外部ネットワーク2を通してクライアントX、クライアントYから伝送される通信データが入力データモニタ11a、11bによって採取される。この入力データモニタ11a、11bによって採取された通信データは推論エンジン12で検出される。

【0015】この推論エンジン12には、あらかじめサーバA～Nへの攻撃パターンが記憶されており、推論エンジン12が入力データモニタ11a、11bによって採取された通信データを検出すると、その検出した通信データのパターンと攻撃パターンとのマッチングの有無を検出する。この際、入力データモニタ11a、11bによって採取された通信データから攻撃パターンらしい通信データが検出されるまで上ステップS1の処理の実行を繰り返す。

【0016】推論エンジン12は、入力データモニタ11a、11bによって採取された通信データの検出中に、この通信データのパターンが攻撃パターンにマッチングすることを検出すると、ステップS2で推論エンジン12はトラフィックシェーパ13に対して、攻撃パターンが検出されたことを通知する。トラフィックシェーパ13は、この通知を受けると、トラフィックを α 倍にシェーピングする。

【0017】このシェーピングする状態は、図1におけるクライアントYからサーバAへのアクセスがこれに当たる。このトラフィックシェーパ13はクライアントYからサーバAへの通信データを「1:1」から「1: α 」倍に、また同様にサーバAからクライアントYへのトラフィックを「1: α 」から「 α :1」倍にする。推論エンジン12により検出されたトラフィックが継続している場合であることをステップS3で推論エンジン12が検出すると、ステップS4でトラフィックシェーパ13はトラフィックの割合を減少するか、否かの判断を行い、トラフィックシェーパ13はトラフィックの割合を減少させない場合には、再びステップS3の処理に戻る。

【0018】また、ステップS4において、トラフィックシェーパ13はトラフィックの割合を変更する場合（減少させる場合）には、ステップS5において、既定のトラフィックの割合 ($0 < \alpha < 1$) を変更して、ステップS2の処理に戻る。一方、上記ステップS3において、推論エンジン12は検出した攻撃の発信元からの通信データが終了したことを検出すると、ステップS6で推論エンジン12はトラフィックのシェーピングを

既定値 ($0 < \alpha < 1$) に戻す。

【0019】

【発明の効果】 以上のように、この発明によれば、通信データとあらかじめ推論エンジンに記憶された攻撃パターンとの一致の検出時に、トラフィックシェーピングによって攻撃のトラフィックを減少させるようにしたので、コネクションの保持時間を長くし、サーバ1台あたりの攻撃時間を増加させることができ、1台あたりの攻撃時間を増加させることは、網羅的に攻撃をかけるスキャナなどの攻撃に有効である。また、サーバプログラムを変更する必要がなくなり、一個所で集中的に攻撃の検出を行うため、それぞれのサーバに検出モジュールを導入する必要がなくなる。さらに、シェーピングによる時間稼ぎを行うことで、サーバのログから時間的余裕を持って攻撃の内容を見るこ

とができ、これにより、攻撃の内容に即した対応が可能となる。

【図面の簡単な説明】

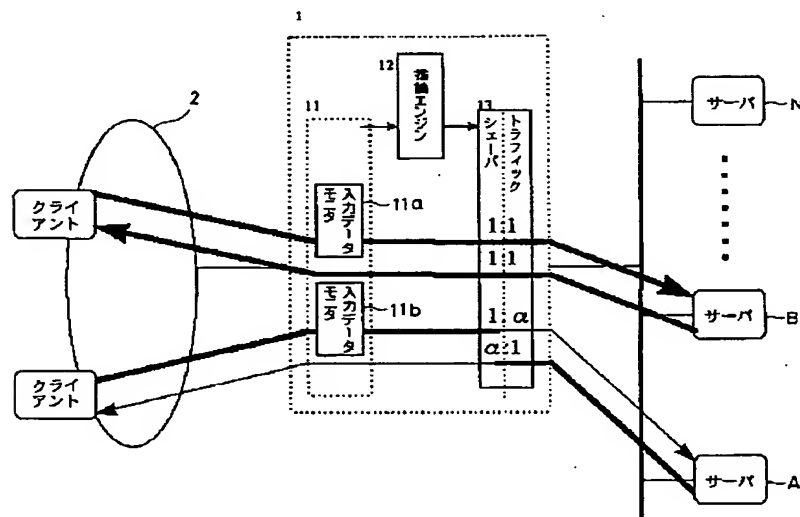
【図1】 この発明によるトラフィックシェーピングによるネットワーク攻撃防御システムに第1実施の形態の構成を示すブロック図である。

【図2】 図1のトラフィックシェーピングによるネットワーク攻撃防御システムの動作を説明するためのフローチャートである。

【符号の説明】

1……防御装置、2……外部ネットワーク、11a、11b……入力データモニタ、12……推論エンジン、13……トラフィックシェーパ、A～N……サーバ、X、Y……クライアント。

【図1】



【図 2】

